Timothy Frese

Honors 190

30 October 2012

The Enigma Machine and Alan Turing

The enigma machine, created by German engineer Arthur Scherbius, was a device used by Germany during World War II to encrypt their communications. This machine was consistently redesigned causing it to be harder and harder to break the code. Allied forces wished to be able to intercept the enemy’s messages, decode them, and be able to better coordinate their war effort in accordance.

Alan Turing, senior code breaker at the British code breaking center at Bletchley Park, is known for creating the theoretical concept of a computer. Turing, working with the allies, created a device named a bombe. This device was able to successfully decrypt German codes and helped to drastically affect the outcome of World War II.

The enigma machine itself is operated by the sender of a message creating a specific setup for the machine. The sender sets the electrical and mechanical settings by arranging the plug wirings and rotor wheels on the device. This setup is known to the sender and receiver. The sender would then type out the message he intended to encrypt. For every letter he typed, the machine would display another letter for him to write down. Eventually, the sender will have written out a string of seemingly meaningless letters. This would be his final encrypted message which would be transmitted via Morse code. These letters would be written down by the receiver and typed back into an enigma machine with the same configuration as the one on which they had been created.

The enigma machine functioned by utilizing the setup chosen by the sender. This setup would determine how the letter gets changed to its encrypted form through a configurable electric circuit. However, this was not the end of the encryption. Every time the user would press a letter to be encoded, the machine would move a rotor and alter the way the next letter was encrypted, causing the code to become exponentially more complex.

Alan Turing’s “Bombe” was able to successfully decode these messages and assist the Allies in predicting German plans. Unfortunately, if the Allies reacted with perfect predictions of their enemy’s plans, the German’s would soon realize their code had been broken and simply switch the setup on their enigma machines. The Allies were forced to only react on some of the information they decrypted in order to keep Germany believing their code was safe.

The Bombe functioned by utilizing a “crib” which was a known (or guessed) word for which they had predetermined what the enigma machine would translate it to. This allowed the Bombe to test large numbers of cases as to what the configuration for the rotors and plugs in the enigma machine could have been. Then, the codebreakers could decrypt and German code they wished.

Winston Churchill has claimed that Turing’s invention of the Bombe was the single greatest contribution to the Allied victory in World War II. Turing’s Bombes were destroyed Churchill’s orders after the war for security reasons. However, the lasting impact of this great invention stays with us. The Bombes helped end the war, and Turing’s contributions are generally credited with creating the field of computer science. This field’s impact is an obvious one on today’s society. Turing’s genius saved lives and set humanity on to a benchmark of technological progress that has defined how our society functions today.